Missouri Statewide Health Information Exchange

Legal/Policy Workgroup

Jefferson City, MO
December 15, 2009
11:00 am – 1:00 pm
Jefferson Building 10th Floor, Conf. Rm. B

MANATT
HEALTH
SOLUTIONS

Agenda

Topic	Facilitator(s)	Time
Welcome & Introductions	Co-Chairs	11:00 – 11:15 am
Overview of Key Privacy & Security Issues	Co-Chairs & Manatt	11:15 – 11:30 am
Process for Developing Privacy & Security Policies	Co-Chairs & Manatt	11:30 – 11:45 am
Consent – Discussion	Co-Chairs & Manatt	11:45 – 12:45 pm
Next Steps		12:45 – 1:00 pm

Welcome & Introductions

Governor Nixon’s Remarks & Vision

- **This is a tremendous opportunity for Missouri – to improve the affordability, quality and value of health care.**
- **It is also an opportunity to bring new investment to Missouri – potentially close to a billion dollars – to create new jobs and to improve public health**
- **Six objectives**
  - Electronic records can help **reduce costly and preventable medical errors** and avoid duplication of treatments and procedures.
  - HIE can dramatically **improve the coordination of care and the quality of decision-making**, even among health care providers who are miles away from one another.
  - This provides us with an opportunity to **give Missourians more complete, accurate and timely information** with which to make decisions about their own health care.
  - This **makes health information portable**, so that whether consumers are switching providers or become sick while on vacation, their health history is available at the point of care.
  - We believe that if done correctly, promoting the use of standardized electronic health records and interoperable systems with strict safeguards can **improve patient privacy**.
  - Moving from paper records to electronic health records has tremendous potential for lowering administrative costs and thus **making health care more affordable**.
- ***Thank you* for partnering with the state in taking critical first steps in building a new framework for health information technology in Missouri**

Meeting Objectives

ONC Cooperative Agreement FOA:

"Privacy and security of health information, including confidentiality, integrity and availability of information, are integral to fostering health information exchange. States and SDEs must establish how the privacy and security of an individual's health information will be addressed, including the governance, policy and technical mechanisms that will be employed for health information exchange."

1. Review key issues for consideration in development of privacy & security policies.

2. Review process for discussing key issues.

3. Begin discussion of potential consent policies.

Stakeholder Feedback

What We Asked

How should privacy and security issues be addressed to best allow and encourage health information exchange?

What We Heard

- Sufficient mechanisms currently exist to insure privacy and security, but a concerted effort must be made to educate the public as to exactly how those mechanisms guarantee privacy and security of the data.
- We should consider changes in State statutes this spring/fall as well as strong authorization and an opt out approach.
- Consider an 'opt-in' policy for consumers. An 'opt-in' policy, gives consumers more control of their data, highlights why they should value an HIE, and probably raises the security and privacy bar as well.
- We should follow HIPAA compliant procedures.
- Providers should be allowed access to patient data from all places at all times. HIPAA is over-enforced to the detriment of patient care. A secure and widely accessible network is key. Primary care physicians need access to mental health records.
- Should be consistency across the state and ideally across the nation.
- Confidentiality and security of patient information is a major issue for physicians and patients. The public has the most to benefit from the use of EMRs, but they also have the most to lose.
- It seems that each member of the exchange would have to provide HIPAA notification to their patients at a minimum.
- The State should establish a model of trust, based on the Federal NHIN model, with a Data Use and Reciprocal Support Agreement (DURSA) required by all participants in the HIE.
    - The entity requesting private patient information from the HIE should be responsible for ensuring all privacy safeguards have been followed. It should also be accountable for any breaches in privacy or security caused by them. The HIE should be a trusted entity to any organization being asked for private patient information. Each individual provider will need to trust each request from the HIE and respond without validating who requested the information. It will be impossible for each provider to know all of the possible organizations that are requesting information and to implement privacy and security policies for each one of them.
    - Entities choosing to connect to the HIE should pass a certification process and demonstrate that they can sustain adequate safeguards over private patient information, and can ensure security for their systems.
    - Entities choosing to connect to the HIE should adhere to established policies for sharing data. Individual entities should not be able to discriminate. Ultimate decision-making regarding sharing of information should lie with the patient.
- We should survey for ways consumers prefer to access their health information and should offer more than one method. We should offer incentives based on a reduction in deductibles or co-pays for using the method.
- The federal government already has the standards/regulations in place that need to be followed. It is easier for a State to follow the federal guidelines.

Overview of Key Privacy & Security Issues

- Goal: Develop policies governing the exchange of Protected Health Information[1] through Missouri's statewide health information network that will support improvement in patient care while earning and maintaining patient trust.

- Key Policy Areas
  - Consent/ Use & Disclosure
  - Authorization
  - Authentication
  - Access
  - Audit
  - Breach

[1] Protected Health Information means individually identifiable health information (e.g., any oral or recorded information relating to the past, present, or future physical or mental health of an individual; the provision of health care to the individual; or the payment for health care) of the type that is protected under the HIPAA Privacy Rule.

Overview of Key Privacy & Security Issues Cont'd

- **Consent/Use & Disclosure:** What rights should consumers have to decide whether and how to permit the exchange of their PHI through MO's statewide HIE network, and for what purposes may such information be used by those who access it.

- **Authorization:** The process of determining whether a particular individual has the right to access Protected Health Information through MO's statewide HIE network. Authorization is usually based on role-based access standards that take into account an individual's job function and the information needed to successfully carry out a role. Authorization policies should set forth minimum requirements that HIE participants should follow when establishing role-based access standards and authorizing individuals to access information through MO's statewide HIE network.

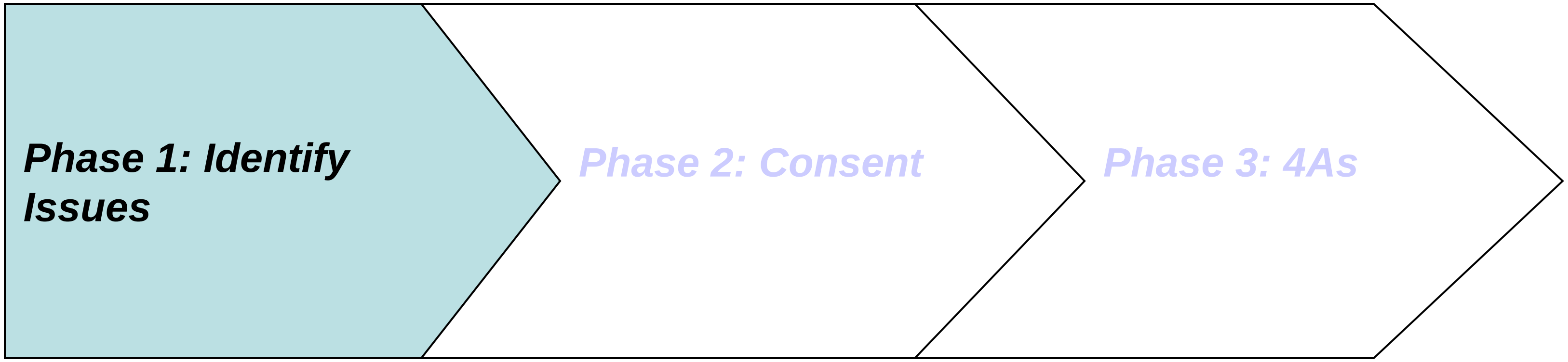
- **Authentication**: The process of verifying that an individual who has been authorized and is seeking to access information via MO's statewide HIE network is who he or she claims to be. Authentication policies represent an important technical security safeguard for protecting a patient's information from various internal and external risks, including unauthorized access. Authentication policies should set forth minimum requirements that HIE participants should follow when authenticating individuals prior to allowing them to access information through MO's statewide HIE network.

- **Access**: Access controls govern when and how a patient's information may be accessed by HIE participants. Access policies should set forth minimum behavioral controls HIE participants should implement to ensure that: 1.) only Authorized Users access information; and 2.) they do so only in accordance with patient consent and with other requirements that limit their access to specified information (e.g., that which is relevant to a patient's treatment).

- **Audits**: Audits are oversight tools for recording and examining access to information (e.g., who accessed what data and when) and are necessary for verifying compliance with access controls developed to prevent/limit inappropriate access to information. Audit policies should set forth minimum requirements that HIE participants should follow when logging and auditing access to health information through MO's statewide HIE network.

- **Breach:** Breach policies are designed to hold HIE participants accountable and to certain behavioral standards when privacy violations occur. Breach policies should set forth minimum standards HIE participants follow in the event of a breach of Protected Health Information through MO's statewide HIE network, assure patients about the RHIO's commitment to privacy, and mitigate any harm that privacy violations may cause.

Process for Developing Privacy & Security Policies



1. **Other Areas to Be Addressed by Legal/Policy Workgroup Upon Completion of Phases 1-3:**
    - Potential modifications to state confidentiality laws and regulations
    - Trust agreements
    - Interstate exchange

2. **Legal/Policy Workgroup will also coordinate with Governance Workgroup on development of a regulatory/enforcement framework to ensure compliance with privacy & security policies.**

Consent

Different Approaches to "Consent"

- ➢ A requirement to obtain patient consent for HIE is not a foregone conclusion.
  - For certain uses (e.g. treatment), some may believe patient consent is unnecessary.
  - Others may believe consumer notification that their information may be exchanged through MO's statewide HIE network will be sufficient.
  - Still others may prefer an opt-out model, in which consumers are given the ability to "opt-out" of having their information exchanged.
  - Finally, some may prefer an "opt-in" model, in which consumers must provide affirmative consent before their information may be exchanged.

- ➢ Potential "Consent" Principles:
  - Promote patient-centered care by facilitating consumer choice and addressing consumer concerns about privacy.
  - Promote exchange of comprehensive information ensuring clinical effectiveness to improve the quality and efficiency of care.
  - Minimize burdens on healthcare providers.
  - Be practical and "implementable" for HIE participants, providing operational flexibility.
  - Be simple and clear .
  - Foster innovation while ensuring public trust.
  - Be technology neutral.

Should Affirmative Consent Be Required for Exchange of PHI through MO's Statewide HIE Network?

- Questions
  - Is affirmative consent necessary under state law?
  - Should it be required in order to earn patient trust and ensure the success of HIE?
  - Should an opt-in or opt-out model be used?

- Considerations
  - Affirmative consent could be useful to provide clear rules in the marketplace for the benefit of consumers, providers and other RHIO stakeholders.
  - Consent policies may update, expand or strengthen state law.

Where and By Whom Should Consent Be Obtained?

- Questions
  - Should consumer consent be obtained prior to "up loading data"? Prior to provider accessing information post-upload?
    - Loading data into a technology platform is a business associate-type arrangement that is not generally considered a "disclosure" requiring patient authorization under HIPAA if the provider holds the data and no other entities have access to it prior to consent.
    - What provisions of Missouri law will impact this issue?
  - Should consumers have the ability to deny access on a provider by provider basis?
  - Should consent obtained by one RHIO participant suffice for all RHIO participants?
  - Should a RHIO be allowed to obtain consent on behalf of participants?

- Considerations
  - Each provider organization could be required to obtain affirmative patient consent to access information through MO's statewide HIE network.
  - Data could be allowed to be "uploaded" prior to receipt of consent to access such data.
  - To ensure that consumers know which health care providers are contributing data to the HIE network, consumers could be given a list of or reference to all data suppliers at the time affirmative consent is granted. Each RHIO could also provide convenient access at all times thereafter, either through its website or otherwise, to a complete and accurate updated list of data suppliers.

Should Sensitive Information Be Filtered or Otherwise Treated Differently?

- Questions
  - Should consumers be able to exclude sensitive information from exchange?
    - Should consumers be able to restrict certain providers' participation in information exchange?
    - Should consumers be able to restrict discrete data elements in information exchange?
    - Should consumers be able to restrict data by encounter?
  - What special protection does MO state law provide for various types of sensitive health information?

- Considerations
  - Allowing filtering of sensitive health information provides protection for consumers.
  - Excluding sensitive health information can compromise quality of care.
  - Excluding sensitive health information could also create financial and operational burdens for HIE participants.
  - Concerns exist about reliability and complexity of restricting information by discrete data elements.
  - Consent to exchange information from designated substance abuse providers is subject to current federal law.

For What Purposes May Information Available through MO's Statewide HIE Be Used?

Treatment

Provider-based quality improvement

Payer-based care management

Research

Marketing

Public health

Law enforcement

Others?

Level 1 Uses?

Level 2 Uses?

Additional Levels?

Potential Definitions of Uses of Information

Treatment

- The provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party. A third party is an entity with whom a health care provider has a contractual relationship related to the provision, coordination or management of health care and related services for a consumer. Under this contractual relationship, the health care provider must ensure that the contracted entity adheres to new consent policies and procedures;
- Consultation between health care providers regarding a patient; and
- The referral of a patient from one health care provider to another.

(Source: Modified from HIPAA)

Provider-based quality improvement

Activities by a provider and/or its contracted entities that include:

- Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination; and
- Disease management which can include a range of activities that involve the provider-controlled exchange of consumer health information with third parties with whom the provider has a contractual relationship related to the provision, coordination or management of health care and related services for a consumer.
- Third party entities may include health plans

(Source: Modified from HIPAA)

Potential Definition of Uses of Information

Payer-based care management

Activities by a health plan that include:

- Conducting case management and care coordination; and
- Disease management which can include a range of activities through which the health plan has direct access to patient-identifiable clinical data without the provider serving as an intermediary.

(Source: Modified from HIPAA)

Research

- A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

(Source: HIPAA)

Marketing

- Any communication about a product or service that encourages recipients to purchase or use the product or service. [1]
- An arrangement whereby an RHIO participant and another entity discloses consumer health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services. [2]

(Source: Modified from HIPAA)

[1] [2] The HIPAA Privacy Rule contains a number of exceptions to marketing that do not require patient authorization. HITECH Section 13406 amended HIPAA such that if a Covered Entity is paid by an outside entity to send a communication to a patient, the communication is deemed to be marketing and requires prior authorization from the patient – even if that communication falls into one of the current exceptions to the definition in the Privacy Rule.

Potential Definitions of Uses of Information

Public health

- Disclosure to a public health authority authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions. *(Source: Modified from HIPAA)*
- Other types of public health disclosures as allowed under HIPAA and state law.

Law enforcement

- Consistent with applicable provisions of HIPAA:
  - Disclosure to a law enforcement official as required by law including laws that require the reporting of certain types of wounds or other physical injuries.
  - Disclosure in response to a law enforcement official's request for PHI for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person.
  - Disclosure in response to a law enforcement official's request for PHI about an individual who is or is suspected to be be a victim of a crime.
- Other types of disclosures as allowed under HIPAA and state law.

(Source: HIPAA)

Should Different Uses of Information Require Different Levels of Consent?

- Questions
  - Should different uses of information require different levels of consent?
  - For uses a consumer may not necessarily anticipate, are more intensive efforts necessary to ensure the consumer understands that they are consenting for these uses of health information?
  - Multiple standards of consent can build patient trust. However, will multiple standards be more burdensome to implement?

- Considerations
  - Some uses of information are likely to be more acceptable and predictable to consumers than others (e.g. treatment, payment as they bring direct personal benefit).
  - Other uses are less likely to be expected (e.g. research and marketing) and may not bring direct personal benefit.
  - Consent requirements for different uses could differ, with a more streamlined process for certain uses and higher restrictions for other uses.

Should Access to PHI Be Permitted in An Emergency Even Absent Patient Consent?

- Questions
  - Should there be "break the glass" capacity?
  - If so, what requirements should be in place to prevent abuse and document appropriate access in emergency situations?
  - What provisions of Missouri law will impact this issue?

- Considerations
  - Break the glass access could be allowed when some or all of the following conditions are met:
    - Emergency situation in which the consumer is unconscious or otherwise unable to give or withhold consent.
    - Treating clinician determines that data that may be available through MO's statewide HIE network may be material to treatment.
    - Consumer has not previously withheld consent for the provider to access his/her data.
    - Physician attests that all of these conditions apply, and Participant maintains a record of access.
    - Others?

How Should Services to Which Minors May Consent Be Handled?

- Questions
  - How does Missouri law address the issue of minors consenting on their own to receipt of sensitive health care services?
  - Are providers required to obtain the minor's consent to disclose information about such services? Are parents prevented from accessing information about such services?
  - Can MO's statewide HIE network ensure that information about such services is exchanged only based on the affirmative consent of the minor and not on a consent previously executed by the minor's parents?

- Considerations
  - Ensuring that information about services for which a minor consented on his or own is only exchanged based on an affirmative consent provided by the minor may require use of technologies to tag and filter such information that are simply not available in the market today.
  - Interim policy solutions may be required to allow at least some group of minors to have their information exchanged, though delineating that group has proven difficult in other states.

Should Standardized Consent Forms Be Utilized across MO's Statewide HIE Network?

- Questions
  - Should a standardized consent form be used across participants in MO's statewide HIE network?

- Considerations
  - A standardized consent form could be developed and approved by the State for use by HIE participants.
  - Standardized consent forms could improve consistency throughout the network but could reduce participant flexibility.

How Durable and/or Revocable Should Consents Be?

- Questions
  - How long should consumer consent last?
  - Are there triggers that require consent to be re-affirmed and if so, what are they?
  - How can a consumer revoke consent?
  - What happens to consumer information once consent is revoked?
  - What provisions of Missouri law will impact this issue?

- Considerations
  - Consent could be for an unlimited period of time but could be revoked at any time.
  - Consent could be time-limited.
  - Revocation of consent could make previously-uploaded data inaccessible, but providers who have already imported a consumer's information into their medical records would continue to have access to such information.

Other Consent Issues for Future Consideration

- Possible exceptions to affirmative consent requirement
  - Public health reporting
  - De-identified data
  - Improvement and evaluation of RHIO operations
  - Disclosures to government agencies for health oversight
  - Others?
- Requests for restrictions on disclosures to payer organizations (new HITECH requirement)
- Others?

Project Milestones & Timelines

Week	Key Topics & Discussions
12/1	➢ Initial kickoff meeting and education ➢ Review charter and project timeline
12/13	➢ Review stakeholder feedback received via web survey to date ➢ Identify key privacy and security issues and process for Workgroup's consideration of issues ➢ Begin discussing issues related to consent and the 4As
1/11	➢ Review draft Strategic Plan language for presentation to Advisory Board ➢ Discuss outstanding questions and identify process for resolution ➢ Continue discussing issues related to consent and the 4As
1/25	➢ Review Advisory Board's feedback and/or questions relative to Strategic Plan ➢ Identify consensus responses to Advisory Board's feedback and Strategic Plan revisions ➢ Continue discussing issues related to consent and the 4As
2/8	➢ Continued working session to finalize Strategic Plan content; incorporate revisions based on Advisory Board's feedback ➢ Identify issues to be "tabled" and to be addressed by the Operational Plan ➢ Continue discussing issues related to consent and the 4As
2/22	➢ Review final Strategic Plan ➢ Review Operational Plan components and requirements ➢ Identify Workgroup milestones and timeline through May ➢ Continue discussing issues related to consent and the 4As

Next Steps

- Workgroup members to submit written feedback to kwallis@manatt.com by Monday, January 4, 2010.
- Workgroup staff to incorporate feedback into development of narrative for Strategic Plan.

Next Meeting: Tuesday, January 12th, 11:30 am – 2:30 pm (Location TBD)

Resources

Missouri Bar Journal Article

"Missouri's Physician-Patient Privilege Presents Problems"

http://www.mobar.org/d518236a-d726-4dc6-bf46-a31ed8c71af8.aspx